Załącznik nr 10 do SIWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa niżej opisanych urządzeń o parametrach technicznych i funkcjonalnych nie gorszych niż wyspecyfikowane.

Przedmiot zamówienia musi pochodzić z legalnego źródła i być przeznaczony do użytkowania w Polsce.

1.1 Urządzenia muszą być fabrycznie nowe i wyprodukowane po 01.0.7.2020 r.

1.2 Urządzenia nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.

1.3 Sprzęt nie może być przeznaczony przez producenta do wycofania ze sprzedaży (nie może mieć ogłoszonej daty wycofania ze sprzedaży).

1.4 Wszystkie oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO 9001

1.5 W momencie oferowania wszystkie elementy oferowanej architektury muszą być dostępne (dostarczane) przez producenta.

1.6 Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, żeby była możliwa identyfikacja zarówno produktu jak i producenta.

1.7 Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych producenta.

1.8 Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej.

1.9 Wszystkie urządzenia muszą posiadać Certyfikat CE produktu.

1.10 Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach : 230 V +/- 10%, 50 Hz.

Adres dostawy Części 1:
Politechnika Warszawska
Dom Studencki Mikrus,
ul. Waryńskiego 10 pok.1 ,
00-631 Warszawa

Adres dostawy Części 2:
Politechnika Warszawska
Pl. Politechniki 1
pok. 320, III p
00-661 Warszawa

2. ZAKRES PRZEDMIOTU ZAMÓWIENIA

Część 1: Dostawa przełączników

1) **Dostawa 12 przełączników z możliwością połączenia w stos;**
2) **Dostawa modułów stack wraz za kablami do posiadanych przez zamawiającego przełączników WS-C2960S-48LPS-L.**

1) DOSTAWA 12 PRZEŁĄCZNIKÓW Z MOŻLIWOŚCIĄ POŁĄCZENIA W STOS

Przełącznik typu stand-alone o parametrach (poniżej podane wartości są minimalnymi):

1. Typ i liczba portów:
   - 48 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + up-link 4x10G SFP+
2. Moc dostępna dla PoE:
   - 740W (z jednym zasilaczem o mocy 1KW),
   - 740W (z dwoma zasilaczami o mocy 1KW pracującymi w układzie redundantnym),
   - 1440W (z dwoma zasilaczami o mocy 1KW pracującymi w układzie współdzielenia mocy),
3. Porty SFP możliwe do obsadzenia następującymi rodzajami wkładek:
   - Gigabit Ethernet 1000Base-T,
   - Gigabit Ethernet 1000Base-SX,
   - Gigabit Ethernet 1000Base-LX/LH,
   - Gigabit Ethernet 1000Base-EX,
   - Gigabit Ethernet 1000Base-ZX,
   - Gigabit Ethernet 1000Base-BX-D/U, -
   - 10Gigabit Ethernet 10GBase-BX-D/U , należy dostarczyć 4 moduły (dwie pary)
   - 10Gigabit Ethernet 10GBase-SR,
   - 10Gigabit Ethernet 10GBase-LR
   - 10Gigabit Ethernet 10GBase-ER,
   - 10Gigabit Ethernet 10GBase-ZR,
   - 10Gigabit Ethernet typu twinax (SFP+ - SFP+) – należy dostarczyć dwa kable o długości 3 M
4. Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
   - Przepustowość w ramach stosu - 80Gb/s,
   - 8 urządzeń w stosie,
   - Zarządzanie poprzez jeden adres IP,
   - Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
   - Wszystkie dostarczone urządzenia musza być dostarczone wraz z modułami i kablami. – dwa kable muszą mieć długość 3 M
5. Zasilanie i chłodzenie
   - Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco" – ang. hot swap),
   - Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia,
   - Redundantne wentylatory,
6. Parametry wydajnościowe:
   - Przepustowość przełącznika (switching capacity):

- 176 Gb/s (bez podłączenia do stosu), 256 Gb/s (z podłączeniem do stosu)
- Prędkość przesyłania (forwarding rate):
- 130.95 Mpps
- Bufor pakietów – 6MB
- Pamięć DRAM – 2GB
- Pamięć flash – 4GB

7. Obsługa:
    - 1000 aktywnych sieci VLAN
    - 16000 adresów MAC
    - 3000 tras IPv4
    - 1500 tras IPv6
    - Ilość wpisów w listach kontroli dostępu Security ACL – 1000
    - ilość wpisów w listach kontroli dostępu QoS ACL – 1000
    - 512 interfejsów SVI L3
    - Jumbo frame 9198B
    - 48 połączeń zagregowanych typu „port channel"
    - 16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP
8. Obsługa protokołu NTP
9. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
10. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    - IEEE 802.1w Rapid Spanning Tree
    - Per-VLAN Rapid Spanning Tree (PVRST+)
    - IEEE 802.1s Multi-Instance Spanning Tree
    - Obsługa 64 instancji protokołu STP
11. Obsługa protokołu LLDP i LLDP-MED.
12. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
13. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
14. Możliwość uruchomienia funkcji serwera DHCP
15. Mechanizmy związane z bezpieczeństwem sieci:
    - Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
    - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
    - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,

- Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
- Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
- Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
- Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
- Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
- Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
- Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
- Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
- Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
- Obsługa list kontroli dostępu (ACL) następujących typów:
- Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
- VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
- Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
- Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
- Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA),
- Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
- Funkcja Private VLAN;

16. Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
    - sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
    - bezpieczna sekwencja uruchamiania,
    - sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
    - Mechanizmy związane z zapewnieniem jakości usług w sieci:
    - Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
    - Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
    - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
    - Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
    - Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),

- Kontrola sztormów dla ruchu broadcast/multicast/unicast,
- Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

17. Obsługa protokołów i mechanizmów routingu:
    - Routing statyczny dla IPv4 i IPv6,
    - Routing dynamiczny – RIP, OSPF do 1000 routes, PIM Stub do 1000,
    - Policy-based routing (PBR),
    - Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup,
    - Obsługa 10 tuneli GRE (Generic Routing Encapsulation);
18. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN
19. Przełącznik musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),
20. Funkcjonalność sondy IP SLA Responder,
21. Zarządzanie
    - Port konsoli,
    - Dedykowany port Ethernet do zarządzania out-of-band,
    - Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
    - Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
    - Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
    - Wsparcie dla protokołu RESTCONF,
    - Przełącznik musi posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
    - Przełącznik musi posiadać wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
    - Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
    - Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki;
22. Możliwość montażu w szafie rack 19”. - zestaw montażowy musi być dostarczony do każdego urządzenia
23. Wysokość urządzenia 1 RU,.
24. Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 16000 strumieni (flow),
25. Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,
26. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
27. Wyposażenie urządzenia

- 10 Przełącznik wyposażony w pojedynczy zasilacz, oraz w moduł do łączenia w stos wraz z kablem stackującym o długości 50 cm
- 2 Przełączniki wyposażone w dwa zasilacze oraz oraz w moduł do łączenia w stos wraz z kablem stackującym o długości 3 m

28. Gwarancja Producenta na okres minimum 36 miesięcy[1] t na poniższych warunkach:
    - Serwis gwarancyjny ma być świadczony w miejscu instalacji,
    - Serwis gwarancyjny musi obejmować dostęp do poprawek oprogramowania w ciągu minimum 36 miesięcy od daty dostawy na żądanie Zamawiającego, nie rzadziej niż raz na 3 miesiące, o ile są one dostępne,
    - Serwis gwarancyjny musi obejmować dostęp do nowych wersji oprogramowania, w ciągu minimum 36 miesięcy od daty podpisania protokołu odbioru'
    - Bieg gwarancji rozpoczyna się w dniu podpisania protokołu odbioru.
    - Firma serwisująca posiada wdrożony i stosowany system zarządzania jakością zgodny z normą ISO 9001 lub normą równoważną na świadczenie usług serwisowych w ramach gwarancji.
    - Wymiana wadliwego sprzętu następnego dnia roboczego od zgłoszenia awarii.

2) Dostawa modułów stack wraz za kablami do posiadanych przez zamawiającego przełączników WS-C2960S-48LPS-L:

- **5 modułów C2960S-STACK**
- **4 kable CAB-STK-E-0.5M**
- **1 kabel CAB-STK-E- 1M**

Część 2: Dostawa dwóch sprzętowych firewalli, które będą pracować jako jeden klaster w układzie podwyższonej niezawodności (High availability):

1) Firewalli;

2) Serwer zarządzania.

1) Firewalli

Nr	Wymagania minimalne
1	Urządzenie musi być dostarczone jako dedykowane urządzenie typu appliance, przystosowane do montażu w szafie Rack 19". Całość sprzętu musi być zarządzana przez jednego producenta.
2	Urządzenie musi być wyposażone w ➢ 4 interfejsy 10GE Ethernet (RJ45) ➢ 16 interfejsów 1/10GE SFP+ obsadzone czterema modułami 10GE SFP+ SR i czterema modułami 10GE SFP+ LR ➢ 4 interfejsy 40GE QSFP+ obsadzone jednym modułem LM4 oraz jednym modułem BIDI

[1] Gwarancja Producenta stanowi kryterium oceny ofert opisane w ust. 3 pkt 2) SIWZ.

	UWAGA – wszystkie moduły (ilości) SFP/QSFP są podane per urządzenie Dodatkowo należy dostarczyć taką sama ilość modułów SFP+ kompatybilnych z kartą liniową do Catalyst 6509 C6800-32P10G będącego w posiadaniu zamawiającego oraz patchcody długości 7m (po 10 naurządzenie): 5xMM LC/SC-PC OM4 i 5xSM LC/SC-PC OM4.
3	Urządzenie musi być wyposażone dedykowany port zarządzania. Port ten musi być wydzielony i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji. Urządzenie musi być wyposażone w moduł Lights Out Management (LOM) lub odpowiednik pozwalający na wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie fizycznym lub sprzętowym (wówczas urządzenie musi zapewniać dedykowane procesory i pamięć dla realizacji modułu zarządzania)
4	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Minimum 16 Gbps dla Firewall/kontroli aplikacji Minimum 8 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware Minimum 150 tys. nowych połączeń na sekundę. Minimum 4.000.000 równoległych sesji Jako scenariusz Firewall/kontroli aplikacji Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych. Jako scenariusz Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych, inspekcje IPS, Antywirus, Anty Spyware. Zakres kontroli musi też obejmować przesyłanie plików do sandboxa lokalnego i chmurowego w tym przechwytywanie i blokowanie plików określonego typu. Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla urządzenia sygnaturami IPS, antywirus i antyspyware.
5	Urządzenie musi umożliwiać działanie co najmniej w trzech trybach pracy • rutera (tzn. w warstwie 3 modelu OSI), • przełącznika (tzn. w warstwie 2 modelu OSI), • w trybie pasywnego nasłuchu (sniffer).
6	Tryb pracy urządzenia musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.)
7	Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3.
8	Urządzenie musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.
9	Urządzenie musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN.
10	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Minimum 10 Gbps dla IPSEC VPN Minimum 5 000 tuneli IPSEC VPN (site-to-site) Minimum 13 000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN. Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji, lub jeżeli dedykowany klient VPN

	(dla Windows, Android, iOS) oferowany przez producenta firewall wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla maksymalnej jego wydajności tzn. dla 13000 jednoczesnych użytkowników
11	Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej ➢ oznaczania pakietów znacznikami DiffServ, ➢ ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. ➢ utworzenia co najmniej 8 klas ruchu sieciowego. ➢ kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. ➢ przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego
12	Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
13	Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.
14	Urządzenie musi obsługiwać nie mniej niż 20 wirtualnych routerów posiadających odrębne tabele routingu.
15	Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych firewalli/systemów/domen/kontekstów i posiadać możliwość rozbudowy do 20 takich systemów. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych: • tablic routingu • Polityk bezpieczeństwa obejmujących i. System IPS ii. System ochrony antymalware/antyspyware iii. System ochrony antywirus • Koncentratorów VPN dla zdalnego dostępu
16	Urządzenie musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu.
17	Urządzenie musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie dla urządzeń. Urządzenia w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active.
18	Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 20 000 reguł polityki bezpieczeństwa oraz obsługę minimum 2000 stref bezpieczeństwa.
19	Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Urządzenie musi wykrywać co najmniej 3000 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.
20	Urządzenie musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM) w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość" w polityce.
21	Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
22	Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie

	rozszerzenia
23	Urządzenie musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji
24	Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download"
25	Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa
26	Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH
27	Rozwiązanie musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o: a) Microsoft Active Directory, b) usługi katalogowe LDAP, c) serwery Terminal Services. d) logi z syslog
28	Polityka kontroli dostępu urządzenia musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
29	Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System IPS musi działać w warstwie 7 modelu OSI. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa) Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi. Zamawiający wymaga dostarczenia licencji na IPS w chwili zakupu urządzenia
30	Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb Baza sygnatur AV musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń Moduł AV musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Zamawiający wymaga dostarczenia licencji na ochronę antywirusową w chwili zakupu urządzenia
31	Urządzenie musi zapewniać ochronę przed atakami typu Spyware – Zamawiający dopuszcza by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik anty-spyware musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby

	funkcja ta była uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza. aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. Zamawiający wymaga dostarczenia licencji na silnik Antyspyware w chwili zakupu urządzenia
32	Urządzenie musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole). Zamawiający nie wymaga dostarczenia licencji na ochronę DNS w chwili zakupu urządzenia
33	Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej
34	Urządzenie musi posiadać funkcjonalność URL Flitering. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 200 milionów rekordów URL. Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania Zamawiający wymaga dostarczenia licencji na URL Filtering w chwili zakupu urządzenia
35	Urządzenie musi posiadać funkcjonalność ochrony przed atakami day zero i współpracy z sandboxem Urządzenie musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box" plików różnych typów co najmniej exe i dll, przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day. Zamawiający nie wymaga dostarczenia licencji w chwili zakupu urządzenia
36	Zarządzanie urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).
37	System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach w szczególności Urządzenie musi mieć zdefiniowane w systemie co najmniej dwa konta typu: a. Administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu b. Operator, który ma możliwość tylko odczytu konfiguracji. Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą • bazy lokalnej, • serwera LDAP,

	• RADIUS lub TACACS+ • SAML 2,0 Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS)
38	Praca na urządzeniu musi odbywać się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian na urządzeniu musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej. Funkcja musi być dostępna co najmniej w interfejsie GUI.
39	Urządzenie musi zapewniać interfejs API (JSON, REST, XML lub inny) będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI)
40	Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. Urządzenie musi mieć możliwość przywrócenia konfiguracji z określnego dnia, w którym były dokonywane zmiany, tzn. po każdym zapisie konfiguracji na urządzeniu powinna być automatycznie zapisywana kompletna konfiguracja, a podczas wyboru konfiguracji musi być widoczna data zapisania konfiguracji.
41	Urządzenie musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall/kontekst wirtualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych, w szczególności niedopuszczalne jest, aby zatwierdzenie zmian w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. w innych systemach wirtualnych
42	Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG.
43	Urządzenie musi być wyposażone w zasilacze typu AC pracujące redundantnie.

2) Serwer zarządzania

Nr	Wymagania minimalne
1	Wraz z urządzeniami Firewall konieczne jest dostarczenie centralnego systemu zarządzania w postaci serwera. Zamawiający dopuszcza budowę systemu w oparciu o kilka komponentów zarządzania oferowanych przez producenta firewalli i systemu zarządzania pod warunkiem, iż będą one pochodziły od jednego producenta i będą przez niego w całości serwisowane. Zamawiający wymaga jednocześnie, aby wymagania dotyczące ➢ Platformy sprzętowej (interfejsy, przestrzeń dyskowa, zasilanie) ➢ liczby zarządzanych firewalli, ➢ wydajności dotyczącej obsługiwanych zdarzeń były spełnione przez każdy z komponentów tworzących system zarządzania. Jeżeli producent rozwiązania zapewnia tylko system zarządzania w postaci maszyny wirtualnej wówczas Zamawiający dopuści takie rozwiązania przy założeniu jego instalacji na serwerach o parametrach rekomendowanych przez producenta i nie gorszych niż wskazanych w wymaganiach. Zamawiający nie dopuszcza oferowania rozwiązań wirtualnych, jeżeli producent zapewnia o ofercie dedykowany „management appliance" spełniający wymagania techniczne Zamawiającego.
. 2	System zarządzania, logowania i raportowania musi zostać dostarczony w postaci dedykowanego urządzenia wyposażonego w: ➢ Minimum 4 interfejsy Ethernet 10/100/1000 ➢ Port zarządzania ➢ przestrzeń dyskową na logi o pojemności nie mniejszej niż 12 TB. Przestrzeń ta musi być dostarczona w jako dyski

	pracujące w RAID 1 lub RAID 10 i być efektywnie dostępna na logi (12TB) ➢ Redundantne zasilacze
. 3	System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne ➢ obsługa nie mniej niż 20 firewalli fizycznych ➢ obsługa nie mniej niż 100 firewalli wirtualnych (w rozumieniu wirtualny kontekst/domena/system uruchomiony na dostarczanym firewallu) ➢ obsługa co najmniej 10 000 logów/zdarzeń na sekund
. 4	System zarządzania, logowania i raportowania musi umożliwiać zbieranie logów zdarzeń z systemów firewall. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW. System musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli.
. 5	System zarządzania, logowania i raportowania musi zapewniać narzędzia dla szybkiej i skutecznej analizy informacji w tym co najmniej ➢ umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych. ➢ tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego. ➢ zapisywanie stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób. ➢ tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down"
. 6	System zarządzania, logowania i raportowania musi umożliwiać centralne zarządzanie wieloma firewallami fizycznymi i logicznymi w tym co najmniej: ➢ budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu. >> Lokalnych (dla wybranych firewalli lub logicznych systemów firewalla) >> globalnych (dla grup firewalli lub kilku systemów logicznych wybranych firewalli). ➢ umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery lub logiczne grupy urządzeń umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, wykorzystanie tych samych obiektów). ➢ Pozwalać na tworzenie raportów na podstawie zbudowanych kontenerów lub grup urządzeń ➢ umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium. ➢ umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych. ➢ umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi.
7	System zarządzania, logowania i raportowania musi umożliwiać centralne narzędzia inwentury i audytu oraz zarządzania konfiguracjami w tym co najmniej musi ➢ umożliwiać dystrybucję i zdalną instalację nowych wersji systemu ➢ umożliwiać tworzenie kopii zapasowych zarządzanych firewalli. ➢ umożliwiać dystrybucję i zdalną instalację nowych sygnatur. ➢ umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia/logicznego systemu przed jej zatwierdzeniem. ➢ pozwalać na zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów. ➢ umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby system zarządzania, logowania i raportowania zrozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone ➢ informować o zmianach konfiguracji systemu
8	System zarządzania, logowania i raportowania musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów.

3) Usługa wsparcia technicznego dla ww. urządzeń:

Wymagane jest dostarczenie wsparcia producenta na okres **60 miesięcy** od podpisania Protokołu odbioru, o którym mowa w Załączniku nr 11B do SIWZ stanowiącego Wzór Umowy. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji zgłoszeń gwarancyjny w trybie 24x7.

4) Wymagania dodatkowe dla ww. urządzeń.

Wskazane poniżej wymagania dodatkowe stanowią Kryteria oceny ofert, o których mowa w ust. 14 SIWZ

Nr	Wymagania dodatkowo punktowane – stanowiące Kryteria oceny ofert
1	**Kryterium nr 2** **Integracja z posiadanymi rozwiązaniami bezpieczeństwa** **Ilość przyznanych punktów: 10 pkt**
	Urządzenia muszą być zarządzane z poziomu pojedynczego centralnego systemu zarządzania wraz z posiadanymi przez Zamawiającego rozwiązaniami w zakresie: ➢ Zbieranie i analizowanie logów ➢ Korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: • ruchu sieciowym, • aplikacjach, • zagrożeniach • filtrowaniu stron www. ➢ Tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. ➢ Tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu. **Zamawiający przyzna dodatkowe 10 punktów, jeżeli dostarczony system zarządzania będzie mógł objąć co najmniej urządzenia jednego ze wskazanych producentów urządzeń bezpieczeństwa będących obecnie w użytkowaniu Zamawiającego: Cisco ASA, Palo Alto Networks NGFW**
2	**Kryterium nr 3** **Wartość techniczna:** **1) blokowanie transmisji plików szyfrowanych – 5 pkt** **2) integracja w środowisku wirtualnym Vmware – 5 pkt** **3) funkcję automatycznego pobierania – 5 pkt** **4) funkcje zbierania, archiwizowania i analizowania logów -5 pkt** **Ilość przyznanych punktów: łącznie 20 pkt**
1)	Urządzenie musi pozwalać na blokowanie transmisji plików szyfrowanych co najmniej • Dokumentów office (doc, xls, ppt) • Plików skompresownych (zip, rar) **Jeżeli urządzenie spełnia wymóg – oferta otrzymuje 5 pkt**
2)	System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych

	adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla. **Jeżeli urządzenie spełnia wymóg – oferta otrzymuje 5 pkt**
3)	Urządzenie Firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty. **Jeżeli urządzenie spełnia wymóg – oferta otrzymuje 5 pkt**
4)	W przypadku utraty komunikacji z centralną konsolą zarządzania urządzenie musi pozwalać na ➢ Lokalne zbieranie i analizowanie logów ➢ korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: • ruchu sieciowym, • aplikacjach, • zagrożeniach • filtrowaniu stron www. ➢ tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. ➢ tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu. Urządzenie musi być wyposażone w twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 2 TB **Jeżeli urządzenie spełni powyższe wymogi – oferta otrzymuje 5 pkt**
3	**Kryterium nr 4** **Dojrzałość rozwiązania** **Ilość przyznanych punktów: maksymalnie 10 pkt**
	Zamawiający przyzna dodatkowe: **10 punktów** - jeśli producent oferowanego rozwiązania w postępowaniu był wskazywany w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części („ćwiartce") Leaders w co najmniej jednym raporcie opublikowanym w ciągu ostatnich 18 miesięcy. **5 punktów** – jeśli producent oferowanego rozwiązania w postępowaniu był wskazywany w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części („ćwiartce") Challengers w co najmniej jednym raporcie opublikowanym w ciągu ostatnich 18 miesięcy. **Zamawiający przyzna w tym kryterium maksymalnie 10 punktów.**